Threat Hunting with the Elastic Stack:
Adversary Detection and ATT&CK Defense

DEF CON 28 Blue Team Village Workshop

Copyright © 2020 Ben Hughes and Polito, Inc.

Agenda

- Threat Hunting Overview
- Elastic Stack Overview
- Kibana Crash Course
- Hands-on Lab Exercises

Copyright © 2020 Ben Hughes and Polito, Inc.

Training Team

- **Ben Hughes**
  - Lead Threat Hunter & Director of Commercial Services
- **Jeff Magloire**
  - Lead Threat Hunter & Senior DFIR Consultant
- *Special thanks to the rest of the Polito Inc. team & Blue Team Village crew for their help with workshop prep!*

Copyright © 2020 Ben Hughes and Polito, Inc.

Elastic Stack VM

Download VM from: Blue Team Village GDrive Folder

- VM will be available the morning of the scheduled workshop
- Download & import into VirtualBox or VMware before workshop starts (2 cores, min. 4 GB RAM recommended)
- Latest version of slides & any other workshop materials will also be available here

Logging into the VM:

- Username: hunter
- Password: hunter

Threat Hunting

Tactics, Techniques, and Procedures (TTPs)

Copyright © 2020 Ben Hughes and Polito, Inc.

Threat Hunting Basics

- **Threat hunting…**
  - Is proactive, but benefits from and contributes to reactive security programs (incident response, forensics)
  - Is methodical and repeatable
  - Is based on hypotheses (one approach at least)
  - Can and should take advantage of automation & machine learning, but experienced human analysis is still crucial
  - Maps to each stage of the cyber kill chain, and can ideally detect and help disrupt any stage of an attack
  - Cares about context
  - Benefits from and contributes to threat intelligence
  - Often involves thinking like an attacker to be a better defender

Copyright © 2020 Ben Hughes and Polito, Inc.

IOCs vs. TTPs

- **Indicators of Compromise (IOCs)**
  - Usually atomic items like IPs, domains, hashes
  - Limited value for hunting
  - Relatively easy for attacker to change
- **Tactics, Techniques, and Procedures (TTPs)**
  - Based on adversary behavior during an attack
  - Valuable when understood & mapped to data for hunting
  - Relatively difficult for attacker to change

IOCs and TTPs are interdependent and can both be utilized for threat hunting.

Copyright © 2020 Ben Hughes and Polito, Inc.

ATT&CK Matrix https://attack.mitre.org/

Copyright © 2020 Ben Hughes and Polito, Inc.

Why Elastic Stack for Threat Hunting?

POLITO INC

- SIEMs are generally limited, inflexible, and expensive
- Splunk is powerful, but expensive, can be challenging to scale, and still proprietary
- While not perfect, overall Elastic Stack excels where SIEMs and Splunk tend to fall short:
  - Open source core, modular design, and highly customizable
  - Rapid development cycle – notable new features released in nearly every minor point release
  - Cluster can be easily hosted anywhere and is scalable
  - Can complement or replace Splunk and/or SIEM
  - Elastic Security is steadily maturing

Copyright © 2020 Ben Hughes and Polito, Inc.

The Elastic Stack

Formerly the ELK Stack

Copyright © 2020 Ben Hughes and Polito, Inc.

Elastic Stack

POLITO INC

- **Elasticsearch** - index storage and search backend
- **Logstash** - used to shape logs and ship logs to Elasticsearch
- **Kibana** - GUI frontend for search, visualization, dashboards, reporting and alerting, and Elastic stack cluster management
- **Beats** - Lightweight log shippers that are installed on endpoints
  - Examples: Filebeat, Winlogbeat, Packetbeat

Elastic Stack New Features

- Exciting developments in 7.x versions
- Basic features for securing your cluster (HTTPS, authentication) now free
- Elastic Security
  - Elastic SIEM
  - Elastic Endpoint Security

SIEM

Copyright © 2020 Ben Hughes and Polito, Inc.

Hosting and Installation Options

- On-premises
- Private Cloud
- Public Cloud
  - AWS
  - GCP
  - Azure
  - VPS Providers
- 3rd party "ELK as a service" offerings
- Standalone (bare metal, VM, container)

Copyright © 2020 Ben Hughes and Polito, Inc.

Logs

Copyright © 2020 Ben Hughes and Polito, Inc.

Potential Log Sources (Not Exhaustive List)

Servers
- Web servers
- Application/API servers, dev servers
- Database servers
- File servers, backup/DR servers
- DNS servers
- Domain controllers, AD, ADFS
- VPN gateways, remote access
- Hypervisors

Endpoints
- Laptops, workstations, kiosks, VMs
- AV/EDR/EPP

Network Stack
- Routers, switches, WAPs
- Firewalls, VPN, SSO, WAFs, IDS/IPS, malware sandboxes
- Web proxies, DNS resolvers
- Email servers, spam/phishing filter gateways

Mobile Devices
- MDM, mobile app telemetry

Applications
- Web applications
- COTS applications
- Custom, in-house applications
- Source code repos, dev/staging apps

Cloud / Containerized Infrastructure
- Office 365, Azure Cloud
- AWS, Google Cloud
- VPS providers, serverless app/API providers
- Docker containers, Kubernetes

SIEM/SOAR
- Potentially both a destination and source of logs

Open Source Intel
- Threat indicator feeds
- GeoIP location
- Passive DNS
- Domain registration, whois
- Certificate transparency
- Social media
- Breach dumps

Copyright © 2020 Ben Hughes and Polito, Inc.

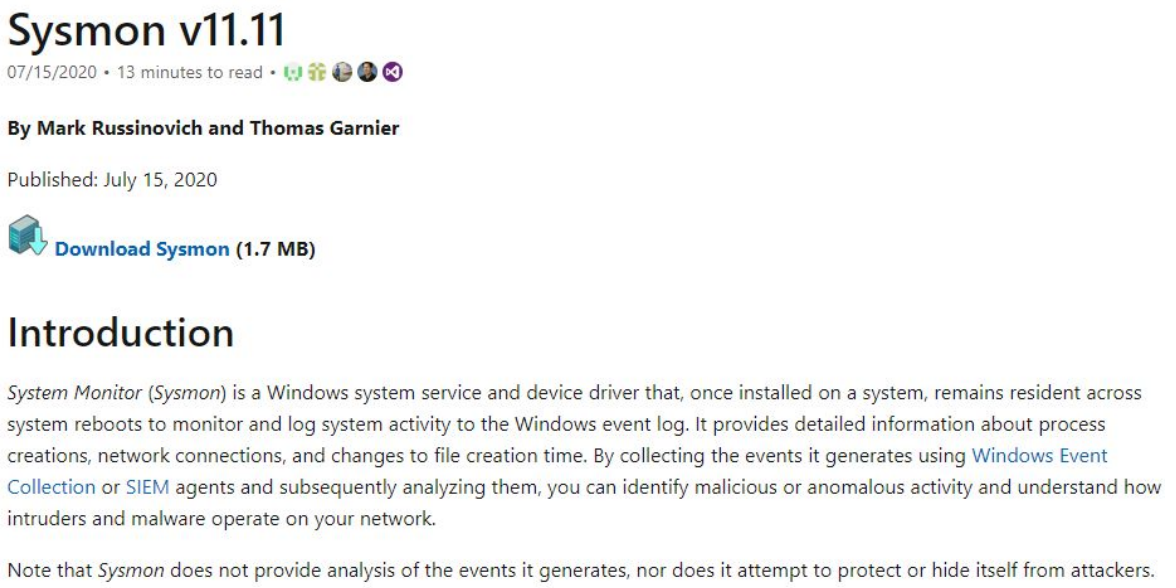
Windows Event Logs

- Even the standard Windows event logs are useful for threat hunting, DFIR, and monitoring. Examples:
  - Login events
  - RDP sessions
  - New services
  - New processes
  - PowerShell and other living off the land TTPs
  - Crashes
  - Logs cleared is itself a notable Windows event…

Copyright © 2020 Ben Hughes and Polito, Inc.

Sysmon

- Free, actively developed Sysinternals endpoint tool from Microsoft
- Kernel level service that monitors & logs all process activity & more
- Available here: https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon



Sysmon v11.11

07/15/2020 • 13 minutes to read •

By Mark Russinovich and Thomas Garnier

Published: July 15, 2020

Download Sysmon (1.7 MB)

Introduction

System Monitor (*Sysmon*) is a Windows system service and device driver that, once installed on a system, remains resident across system reboots to monitor and log system activity to the Windows event log. It provides detailed information about process creations, network connections, and changes to file creation time. By collecting the events it generates using Windows Event Collection or SIEM agents and subsequently analyzing them, you can identify malicious or anomalous activity and understand how intruders and malware operate on your network.

Note that *Sysmon* does not provide analysis of the events it generates, nor does it attempt to protect or hide itself from attackers.

Copyright © 2020 Ben Hughes and Polito, Inc.

Hunting with Sysmon

POLITO INC

Examples of what to look for in Sysmon logs:

- Malware being downloaded and executed
- MS Office macros spawning suspicious processes
- Browser spawning suspicious processes
- Files being deleted or renamed en masse (ransomware?)
- Process injection
- Cross-process activity (lsass.exe's memory being accessed by another process)
- PowerShell and other common "living off the land" TTPs
- Unusual network connections

Copyright © 2020 Ben Hughes and Polito, Inc.

Kibana Crash Course

Kibana Key Features

Copyright © 2020 Ben Hughes and Polito, Inc.

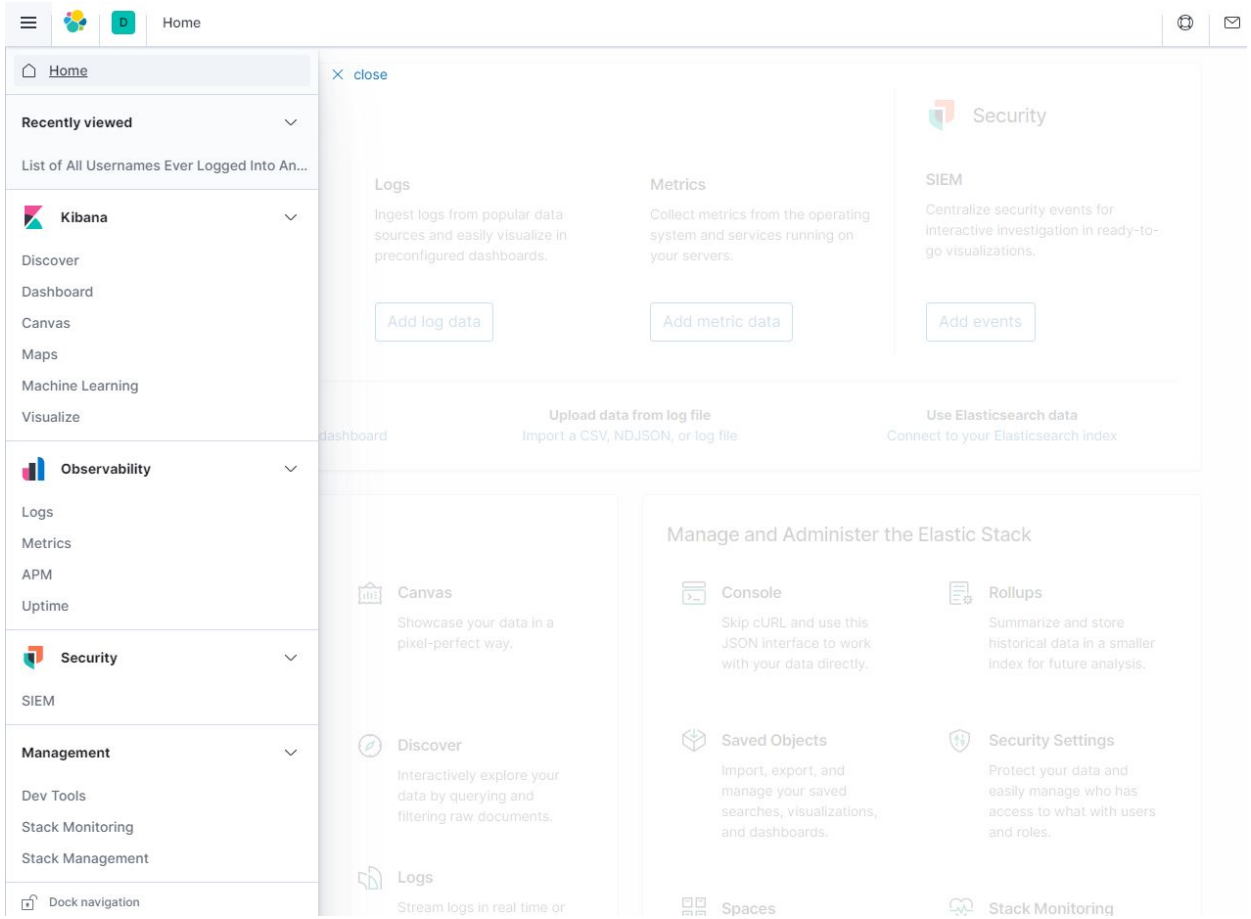
Accessing Kibana in VM

- Browser support – Chrome/Chromium recommended but other browsers like Firefox & Safari are supported too

- Kibana: Port 5601 by default
  - **http://localhost:5601/**
- Elasticsearch: Port 9200 by default
  - **http://localhost:9200/**
- (re)start services if not currently running:
  - **sudo systemctl start elasticsearch.service**
  - **sudo systemctl start kibana.service**

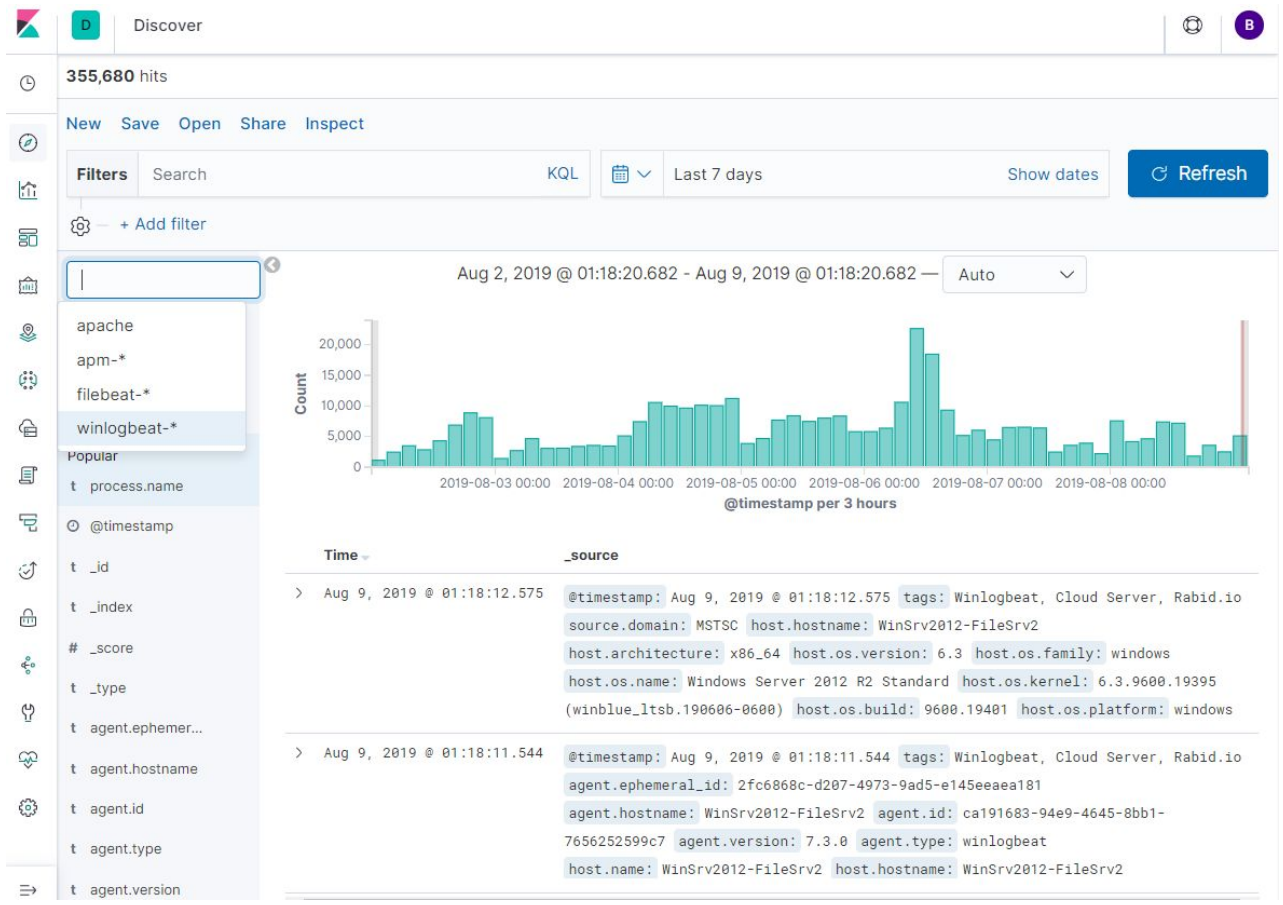
Copyright © 2020 Ben Hughes and Polito, Inc.

Kibana - Home & Dock



Kibana - Key Features

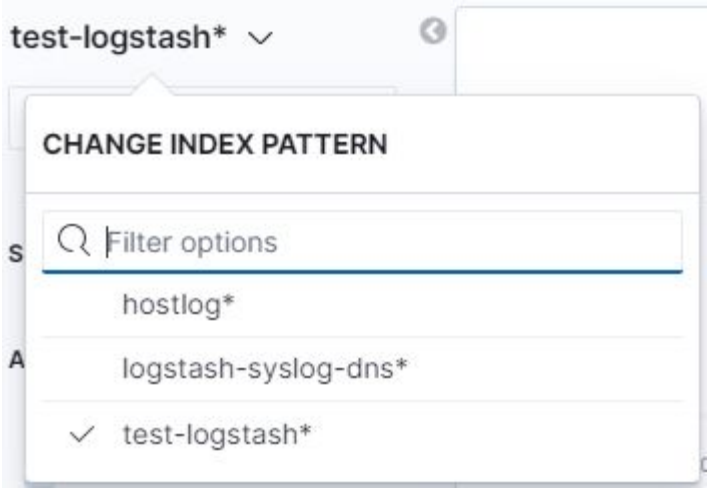
- **Discover (search)**
- **Visualize**
- **Dashboard**


Discover
355,680 hits
New Save Open Share Inspect
Filters Search KQL Last 7 days Show dates Refresh
+ Add filter
apache
apm-*
filebeat-*
winlogbeat-*
Popular
t process.name
@timestamp
t _id
t _index
_score
t _type
t agent.ephemer...
t agent.hostname
t agent.id
t agent.type
t agent.version
Aug 2, 2019 @ 01:18:20.682 - Aug 9, 2019 @ 01:18:20.682 — Auto
Count
20,000
15,000
10,000
5,000
0
2019-08-03 00:00 2019-08-04 00:00 2019-08-05 00:00 2019-08-06 00:00 2019-08-07 00:00 2019-08-08 00:00
@timestamp per 3 hours
Time
_source
Aug 9, 2019 @ 01:18:12.575
@timestamp: Aug 9, 2019 @ 01:18:12.575 tags: Winlogbeat, Cloud Server, Rabid.io source.domain: MSTSC host.hostname: WinSrv2012-FileSrv2 host.architecture: x86_64 host.os.version: 6.3 host.os.family: windows host.os.name: Windows Server 2012 R2 Standard host.os.kernel: 6.3.9600.19395 (winblue_ltsb.190606-0600) host.os.build: 9600.19401 host.os.platform: windows
Aug 9, 2019 @ 01:18:11.544
@timestamp: Aug 9, 2019 @ 01:18:11.544 tags: Winlogbeat, Cloud Server, Rabid.io agent.ephemeral_id: 2fc6868c-d207-4973-9ad5-e145eeaea181 agent.hostname: WinSrv2012-FileSrv2 agent.id: ca191683-94e9-4645-8bb1-7656252599c7 agent.version: 7.3.0 agent.type: winlogbeat host.name: WinSrv2012-FileSrv2 host.hostname: WinSrv2012-FileSrv2

Copyright © 2020 Ben Hughes and Polito, Inc.

Kibana - Discover

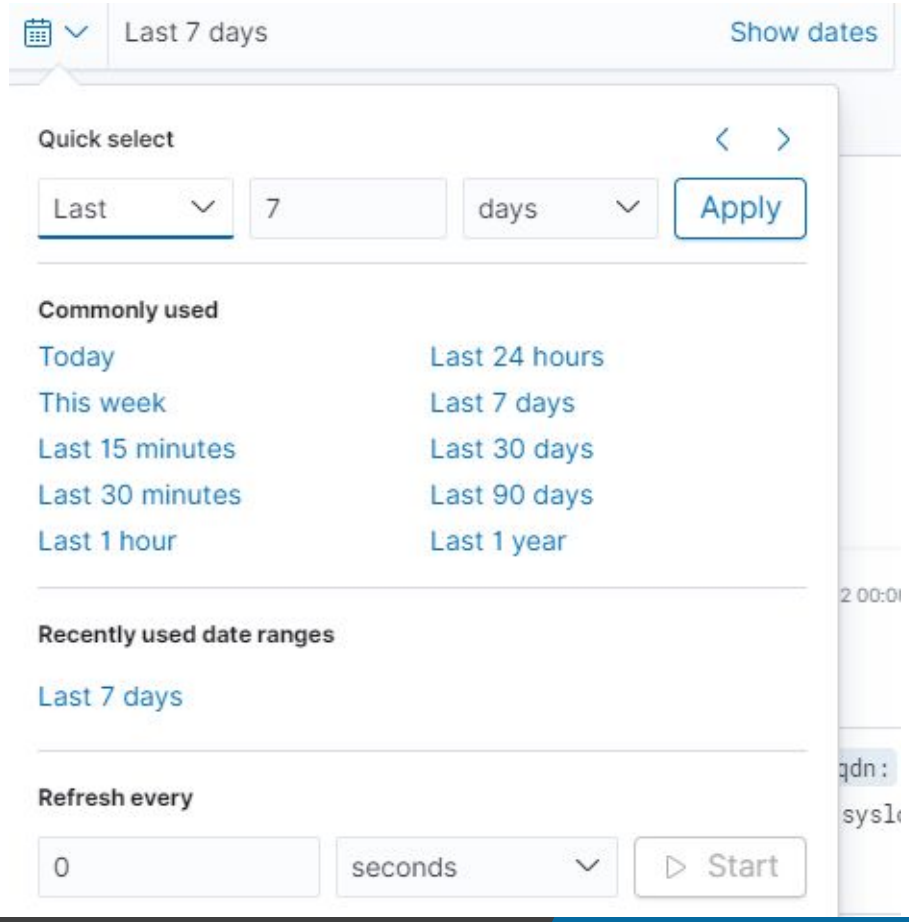
- **Index Pattern Filter**
  - Examples:
    - filebeat-* indices
    - logstash-* indices
    - winlogbeat-* indices



Copyright © 2020 Ben Hughes and Polito, Inc.

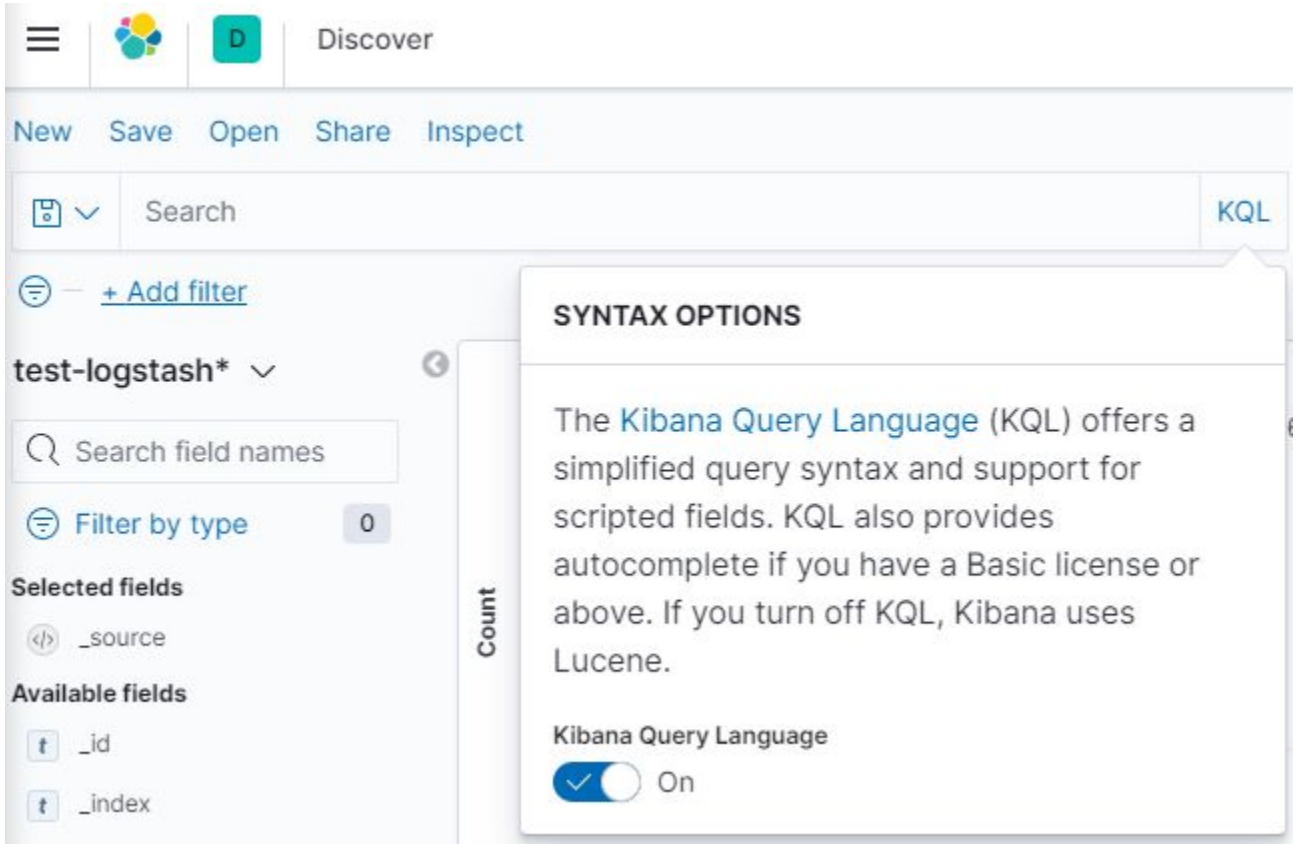
Kibana - Discover

- **Time Range Filter**



Copyright © 2020 Ben Hughes and Polito, Inc.

Kibana - Search (KQL)

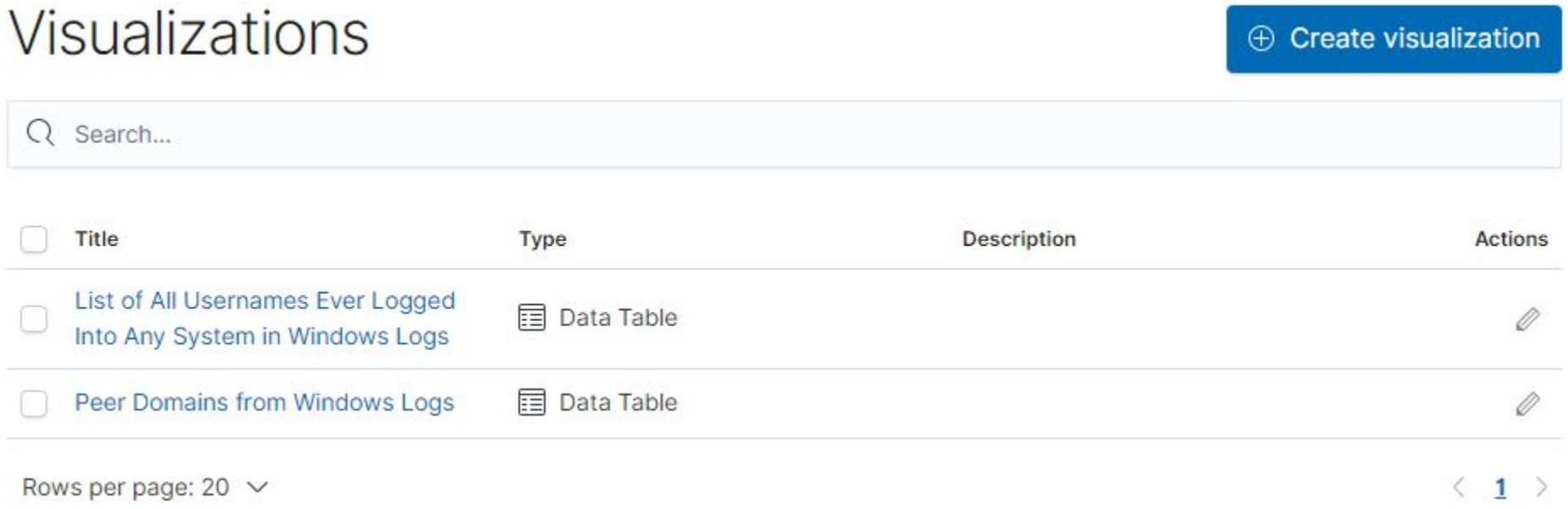


Kibana - Search

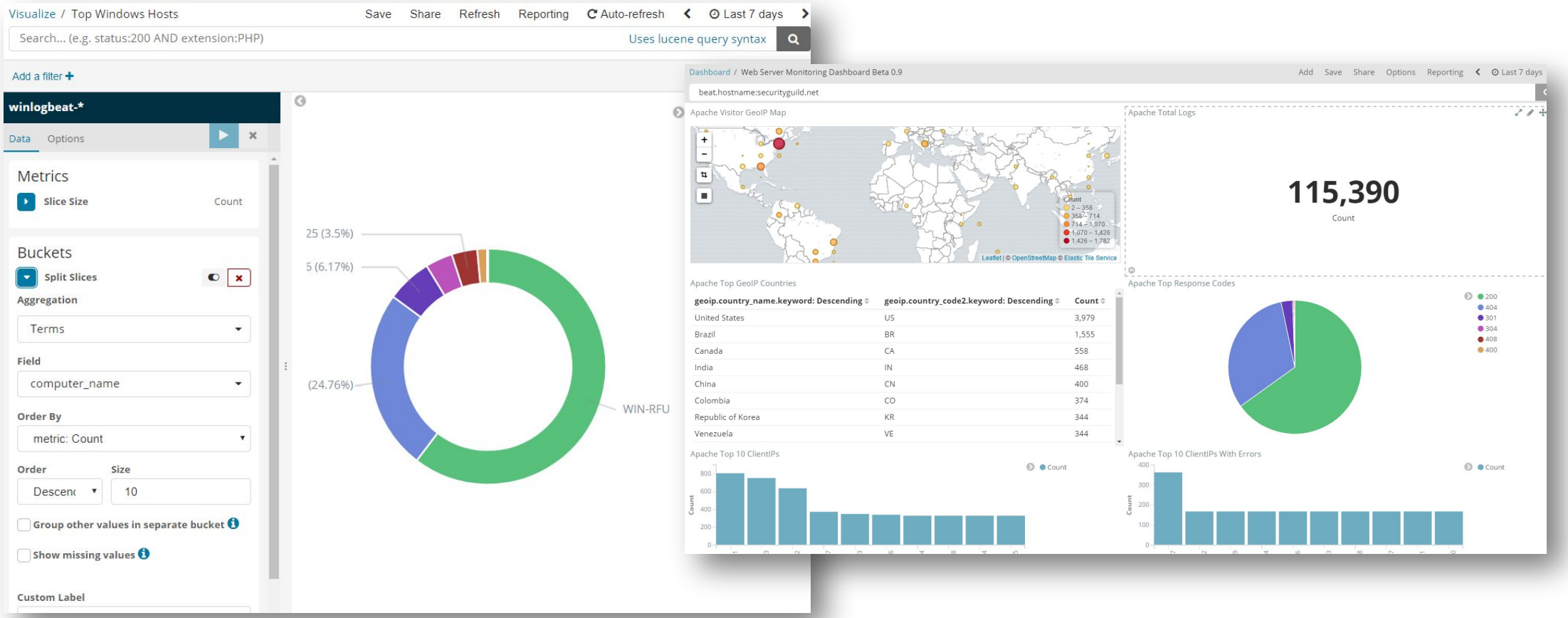
- Default search syntax based on Kibana Query Language (KQL)
- Format is: FieldName:SearchTerm (autocomplete is helpful)
- Fields & search terms can be Case Sensitive
- Boolean operators like AND, OR & nested statements are supported
- * wildcards can be used, but use sparingly
- Free text searches can be used, but use sparingly
- Example searches:
  - computer_name:ACME-SRV2008-DC
  - process.command_line:*powershell.exe*
  - "urgent_invoice.docm"

Copyright © 2020 Ben Hughes and Polito, Inc.

Kibana - Visualize



Visualizations

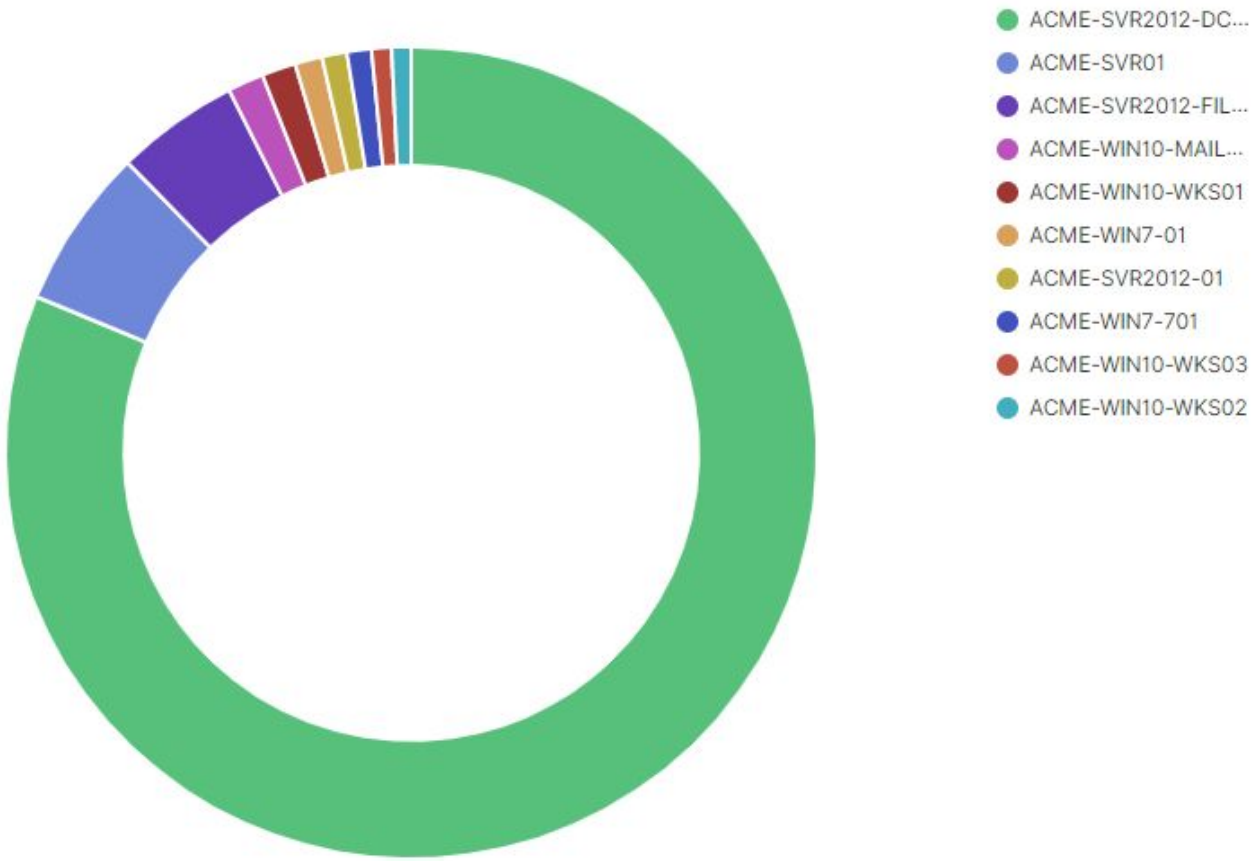


Copyright © 2020 Ben Hughes and Polito, Inc.

Visualization Lab #1

Pie Chart:

Top Hostnames



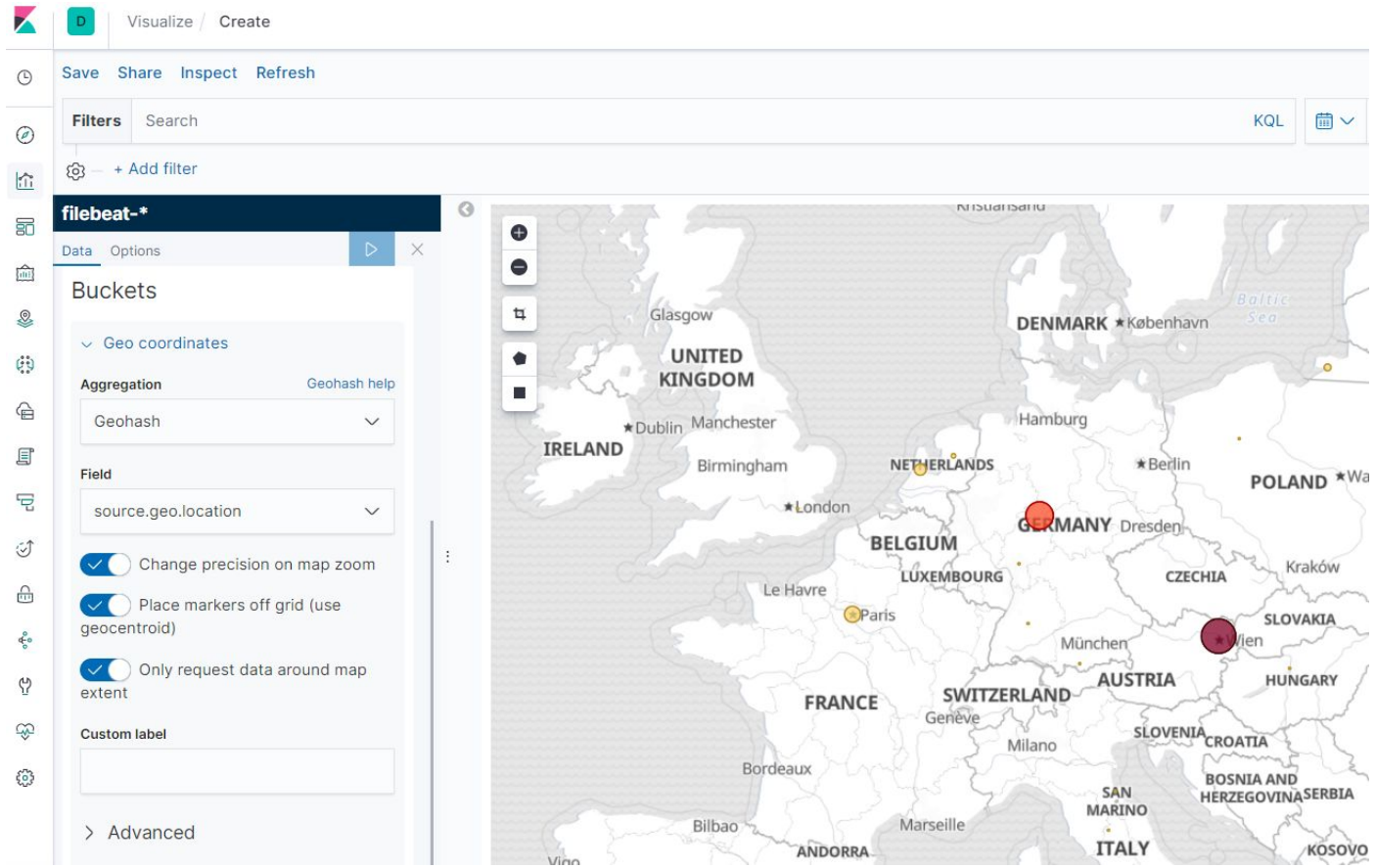
Visualization Lab #2

POLITO INC

Data Table: Rare EXE Hashes

hash.sha1: Ascending	process.executable: Ascending	winlog.computer_name: Ascending	Count
01d5c03be3573d32ed6f0754b903a0c0b05825db	C:\Windows\System32\runonce.exe	ACME-WIN7-01	1
0230276ac0f21520c449a0415b1f1d4acdfda894	C:\Windows\System32\msinfo32.exe	ACME-WIN7-701	1
0576f01c2a0b950b2ceb35b85432a239314a353a	C:\Users\djackson\Downloads\UPS\DrbUih.exe	ACME-WIN10-WKS03	1
0a8859c9d27504145b834ffffcc11ad674ef8b04	C:\Program Files\Windows NT\Accessories\wordpad.exe	ACME-SVR2012-DC01	1
0b112a496706768428e4e0f3f58a6f0e3a1cb8c9	C:\a7a23746-96fd-4191-b40b-95bc1095b1f5.exe	ACME-WIN7-02	1
0f59b56fd37b75f7f20df5a78c429cde8790f550	C:\Windows\System32\wbem\mofcomp.exe	ACME-WIN7-01	1
0f6b5dd7a093fa00ef0a984af3e447a07d0d9630	C:\Windows\System32\WinBioPlugIns\FaceFodUninstaller.exe	ACME-WIN10-WKS01	1
104463a5d7cbafa8676276e8caa500908422b10e	C:\Windows\servicing\TrustedInstaller.exe	ACME-WIN10-MAILROOM	1
106435723da8f480796c3aaa8241b04c3db35a6e	C:\Windows\System32\Sysprep\sysprep.exe	ACME-SVR2012-01	1
1a7f8783f3e59716720482af29f1dd784b298f24	C:\Program Files\WinZip\WzPreviewer32.exe	ACME-WIN7-02	1

Map (GeoIP) Visualization



Copyright © 2020 Ben Hughes and Polito, Inc.

Kibana - Dashboard

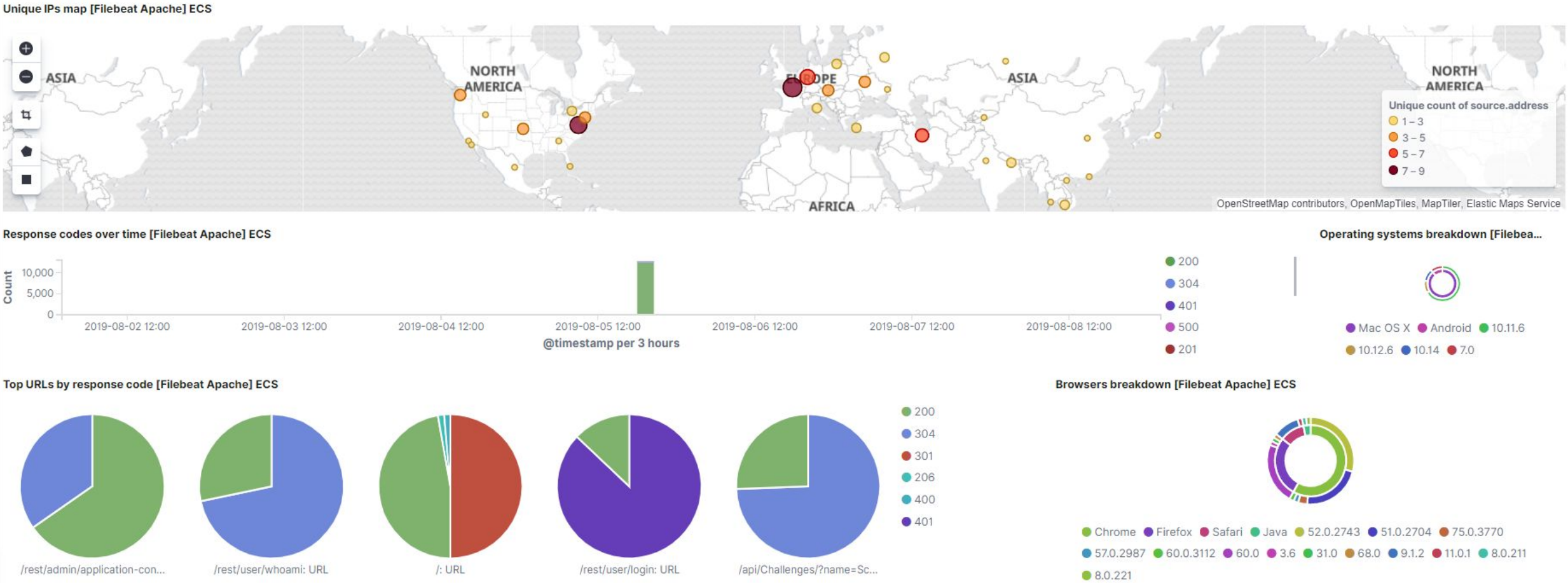
Create your first dashboard

You can combine data views from any Kibana app into one dashboard and see everything in one place.

New to Kibana? Install some sample data to take a test drive.

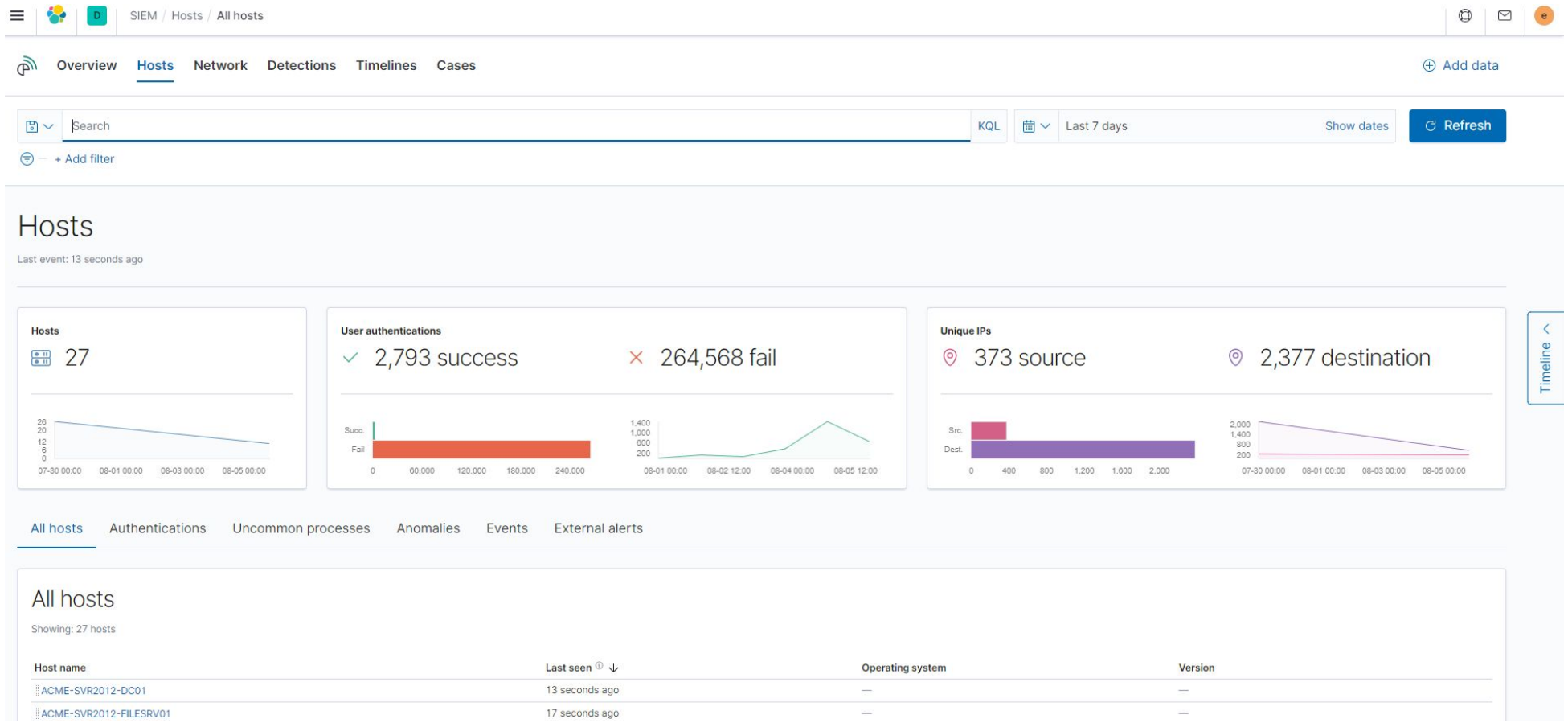
⊕ Create new dashboard

Kibana - Dashboard



Copyright © 2020 Ben Hughes and Polito, Inc.

Elastic SIEM



Copyright © 2020 Ben Hughes and Polito, Inc.

Elastic SIEM

- Free in 7.x
- Work in progress – currently supported data types and detection rules are limited, new features being added
- Can accelerate or complement simple SIEM use cases
- Not (yet) a full replacement for building out custom Kibana queries, visualizations, and dashboards
- https://www.elastic.co/products/siem
- Also in development: Elastic Endpoint Security (based on Endgame integration)

Copyright © 2020 Ben Hughes and Polito, Inc.

Let's Go Hunting

Sample Hunts in Kibana

Copyright © 2020 Ben Hughes and Polito, Inc.

Hunting for Suspicious Windows Events

POLITO INC

Common Examples:

- Credential attacks, credential dumping
- Unauthorized RDP login
- Lateral movement
- Living off the land binaries and scripts (LOLBAS)
- Malicious Office macros
- Malicious PowerShell
- Botnet & trojan infections
- Ransomware
- Command and Control (C2) traffic
- Sensitive data exfiltration
- Log tampering

Hunt #1 - Credential Attacks

What host has been the victim of the most credential attacks this week?

- Hint #1: Use Discover or Visualize
- Hint #2: What Event ID represents unsuccessful logon attempts?

Solution: [redacted]

Hunt #2 - RDP

What host has the most successful remote interactive logins this week?

- Hint #1: What Event ID represents successful account logged on events?
- Hint #2: What Logon Type for that Event ID represents Remote Interactive logons?

Solution: [redacted]

Hunt #3 - RAT

What host had a popular remote access tool installed & used on Aug. 6?

- Hint #1: Search for popular remote access tools (RATs)
- Hint #2: An unauthorized individual may have initiated a remote session to this host using this RAT, using suspicious source IP 74.119.146.35

Solution: [redacted]

Living Off the Land (LOL)

- Abuse of PowerShell, WMI, PSExec, MSHTA, wscript, Sysinternals, etc. is common
  - Hunting for obfuscated PowerShell is an easy win
  - Hunting for rare scripts and command lines is an easy win
  - As always, depends on log data visibility; e.g. are you logging full PS scripts in your environment?
- Living Off the Land Binaries and Scripts (LOLBAS)
  - Many examples: https://lolbas-project.github.io
  - Can map to ATT&CK TTPs

Copyright © 2020 Ben Hughes and Polito, Inc.

Hunt #4 - Cred Dump

On what host did an attacker dump hashes from memory using a popular Windows Sysinternals tool and what was the command used?

- Hint #1: the attacker used procdump
- Hint #2: dumping the memory contents of the Windows process lsass.exe is a common attacker technique to obtain hashes (and in some cases cleartext creds) that can be cracked offline

Solution:

[redacted]

Hunt #5 - PowerShell 1-liner

Find an example of a malicious PowerShell script that an attacker executed to download and run a popular credential attack tool on a server.

- Hint #1: Look for rare PowerShell command lines
- Hint #2: Look for Mimikatz

Solutions:

[redacted]

Hunt #6 - PUPs

What user downloaded and installed multiple Potentially Unwanted Programs (PUPs) on Aug. 4?

- Hint #1: A popular BitTorrent client was the first PUP, which likely led to others
- Hint #2: A fake driver installer and fake browser security extension were also installed

Solution: [redacted]

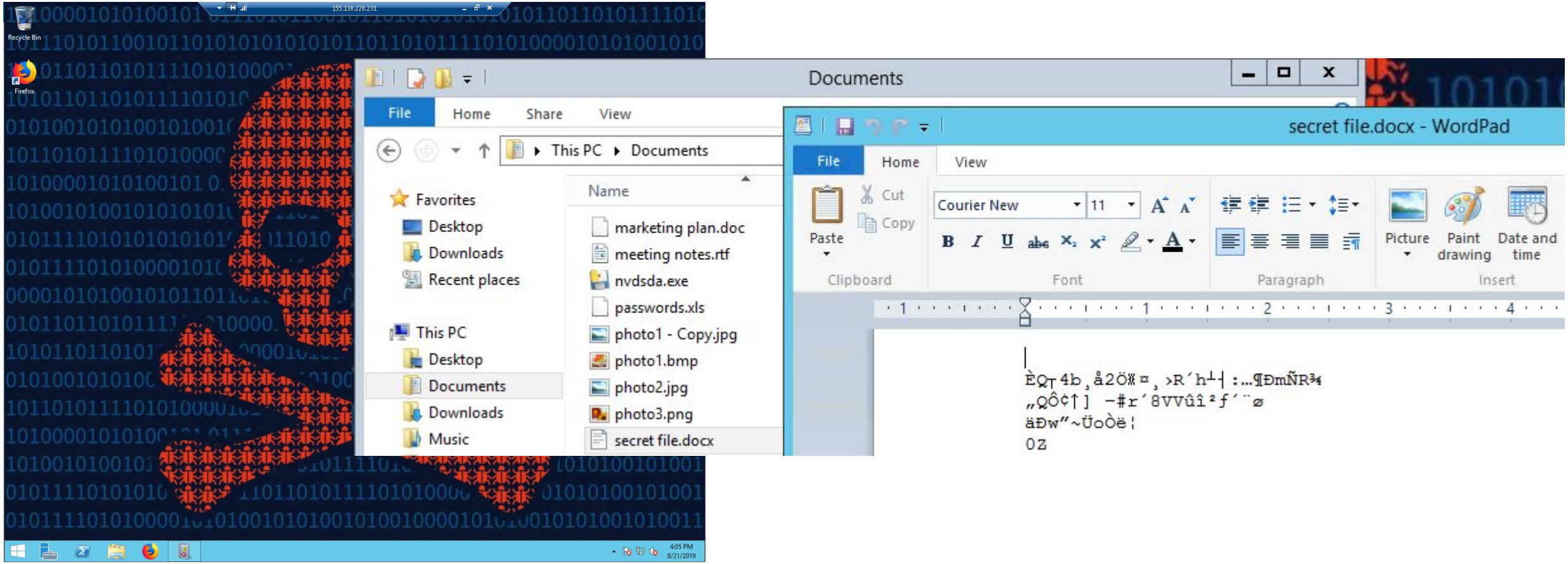
Hunt #7 - maldoc

What is the name of the malicious document that ran obfuscated PowerShell when the phishing victim opened it and presumably enabled macros on Aug. 5?

- Hint #1: The host was ACME-WIN10-WKS03
- Hint #2: "-Enc" is a common PowerShell parameter that attackers use to Base64 encode their scripts

Solution: [redacted]

Ransomware:
Many Opportunities for Early Detection



Copyright © 2020 Ben Hughes and Polito, Inc.

Hunt #8 - Prelude to Ransomware

What hosts had their volume shadow copies deleted and what command(s) were used? Ransomware operators often do this to prevent such backups from being restored.

- Hint #1: 2 hosts involved
- Hint #2: vssadmin is a Windows utility for managing volume shadow copies

Solutions:

[redacted]

Hunt #9 - Ransomware

The IR team has identified a ransomware SHA1 hash that started to actively propagate across your network overnight on Aug. 5: **28896a2fb5e8e5961ae61df9b0c34b31f6d6bf70**. What are the full paths to EXEs matching that hash on a server?

- Hint #1: Sysmon hashes EXEs during related disk operations and executions; multiple fields may contain the relevant hash
- Hint #2: The most recent ransomware infection happened on ACME-SVR2012-DC01.

Solution:

[redacted]

Hunt #10 - Log Tampering

On what host(s) did an attacker clear Windows event logs, and what log channel was cleared?

- Hint #1: There is a specific Event ID for "the audit log was cleared"
- Hint #2: The relevant Event ID was logged on Aug. 2 and Aug. 5

Solution:

[redacted]

Hunt #11 - Targeted Accounts

What were the top usernames for failed login attempts on Aug. 4?

- Hint #1: What Event ID represents failed logon attempts?
- Hint #2: Can use Discover's Top 5 values for the relevant username field, or a visualization with Descending order set to Size 5 may help
- Hint #3: Remember to set the time range filter to only include Aug. 4

Solution:

[redacted]

Hunt #12 - C2 IP

On Aug. 2, what C2 IP address did suspicious process "ssss.exe" connect to?

- Hint #1: What Sysmon Event ID covers network connections?
- Hint #2: What field includes destination IPs?

Solution:

[redacted]

Hunt #13 - C2 Domain

On Aug. 5, what process beaconed out to vps001[.]reestyle[.]net for C2, and what is the associated IP?

- Hint #1: What Sysmon Event ID covers network connections?
- Hint #2: ACME-WIN7-706 is the infected host

Solution:

[redacted]

Hunt #14 - Ransomware Redux

POLITO INC

- While restoring an old backup, a user was accidentally reinfected with an old Petya ransomware variant. What is its EXE name?
  - Hint #1: The reinfected host is ACME-WIN7-707
  - Hint #2: https://www.virustotal.com/gui/file/4c1dc737915d76b7ce579abddaba74ead6fdb5b519a1ea45308b8c49b950655c/detection

Solution:

[redacted]

Hunt #15 - Different RAT

On Aug. 1, a Remote Access Trojan (RAT) ran on an infected host and created a firewall rule to allow its traffic; what is its full path?

- Hint #1: The host is ACME-WIN7-715
- Hint #2: The RAT used a "netsh" command.

Solution:

[redacted]

Additional Hunts

There are other malicious events in this Windows log data set. Hone your threat hunting skills in Kibana and find as many of them as you can!

Wrapping Up

How to Continue the Hunt

Copyright © 2020 Ben Hughes and Polito, Inc.

Suggested Next Steps

- Additional training and events
  - CTFs like OpenSOC (here at Blue Team Village!)
- Deploy Elastic Stack for yourself
  - Elastic Cloud 14-day free trial: https://www.elastic.co/cloud/elasticsearch-service/signup
  - Install in a VM or container
- Try a security-focused Elastic Stack distro like Security Onion and HELK
- Try Sysmon with a sample config
- Explore the many projects related to log data-driven threat hunting
- Practice identifying attacker TTPs, mapping to ATT&CK, running attack simulations, and determining detection potential/gaps

Copyright © 2020 Ben Hughes and Polito, Inc.

References

- Elastic Stack
  - https://www.elastic.co/guide/en/elastic-stack/current/installing-elastic-stack.html
  - https://www.elastic.co/cloud/elasticsearch-service/signup
  - https://www.elastic.co/downloads/beats/winlogbeat
  - https://www.elastic.co/beats/filebeat
  - https://www.elastic.co/siem
  - https://github.com/elastic/detection-rules
- Sysmon: https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon
- MITRE ATT&CK Framework: https://attack.mitre.org/
- Windows Event ID References:
  - https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/
  - https://www.malwarearchaeology.com/cheat-sheets

Credits

- Blue Team Village Crew
- The rest of the Polito Inc. team
- Elastic and Elastic Cloud
- Elasticdump:
  - https://github.com/elasticsearch-dump/elasticsearch-dump
- Mark Russinovich & Microsoft
  - Makers of Sysmon
- @malware_traffic https://www.malware-traffic-analysis.net/
  - Source of malware samples & analysis

Copyright © 2020 Ben Hughes and Polito, Inc.

Contact us with any questions!

E-mail
info@politoinc.com

Website
www.politoinc.com

Blog
www.politoinc.com/blog

Twitter
@politoinc

GitHub
www.github.com/politoinc

Trainers:

Ben Hughes
ben@politoinc.com
@CyberPraesidium

Jeff Magloire
jeff@politoinc.com

Copyright © 2020 Ben Hughes and Polito, Inc.